BY ORDER OF THE COMMANDER
AIR FORCE RESERVE COMMAND

AIR FORCE RESERVE COMMAND
INSTRUCTION 14-101

10 July 2000

Intelligence

AFRC THREAT WORKING GROUP

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AFRC WWW site at: http://www.afrc.af.mil and the AFRCEPL (CD-ROM) published monthly.

OPR: HQ AFRC/DOIO (Lt Col Eugene V. Ziemba JR.)

Certified by: HQ AFRC/DOI
(Col Joseph Molyson)
Pages: 21
Distribution: F

This instruction implements AFPD 14-1, *Intelligence Applications and Requirements Planning*, and prescribes guidelines for the Threat Working Group operating at the headquarters and unit levels. It assigns responsibility for managing the process.

1. Threat Working Group:

1.1. Charter:

1.1.1. The AFRC Threat Working Group (TWG) provides HQ AFRC and all AFRC units with a single focal point for coordinated all-source threat analysis for ongoing and future operations.

1.1.2. Weekly TWG meetings combine intelligence, operations, counterintelligence, security, and force protection functions in one comprehensive working group to develop risk assessments and force protection recommendations.

1.2. Membership:

1.2.1. TWG principal membership includes representatives from DOI, DOCC, DOOM, DOOX, SF, SG, and AFOSI Region 3/OL-B.

1.2.1.1. A principal and/or at least one action officer for each functional area attend the TWG meetings.

1.2.1.2. The TWG is on call to DOCC 24-hours a day.

1.2.1.3. Other internal and external AFRC organizations support the TWG with products, services and inputs on an as needed basis.

1.3. Processes:

1.3.1. The TWG meets to discuss current and potential threats affecting AFRC planning and operations.

1.3.1.1. AFRC/DOOM notifies TWG members of AFRC missions outside the continental United States.

1.3.2. The TWG reviews Secure Launch Country List (AMC, USAFE).

1.3.3. AFRC/DOIO intelligence briefs on significant, current developments potentially impacting AFRC operations worldwide.

1.3.4. The TWG identifies airfield locations or facilities requiring force protection reviews, risk assessment, and/or briefing.

1.3.4.1. TWG action officers develop and coordinate risk assessments and develop force protection recommendations. Action officers also identify missions requiring Raven Team deployments.

1.3.4.2. TWG principals review and approve risk assessments and recommended force protection measures.

1.3.4.3. TWG passes force protection recommendations to appropriate command decision-makers.

1.3.5. The TWG accepts force protection recommendations made in-theater or from Air Mobility Command (AMC).

1.3.5.1. The AFRC TWG adopts AMC or USAFE TWG recommendations as is.

1.3.5.2. In the event that a conflict between command (for example, AMC or USAFE TWG) recommendations occurs, adopt the more restrictive recommendations.

1.3.6. The TWG uses the risk management tools in attachments 6 and 7 to determine force protection recommendations.

1.3.7. AFRC's TWG program complies with higher headquarters' guidance, policy, and doctrine.

1.3.7.1. AFRC's Force Protection Board, which is a policy making forum that reviews high level force protection issues such as funding, training and manpower, may task the TWG to staff FP-related issues.

1.4. Products:

1.4.1. TWG action officers produce written risk assessments and briefing products on airfields and specific geographic regions as well as recommendations for force protection. TWG products include:

1.4.1.1. The TWG Report: produced weekly based on evaluation of AFRC missions and deployments. Area threat and suggested countermeasures (attachment) are included.

1.4.1.2. Operation Risk Management Matrix (Attachment 6, Figure A6.1): Classified document, which evaluates the overall terrorist, military, and criminal threats and the force protection, mitigating measures. Forms primary baseline to determine "GO/NO GO" for individual missions.

1.4.1.3. Risk Assessment (Attachment 7, Figure A7.1): Published classified analysis that details terrorist, military, criminal, medical and information warfare (IW) threats and force protection recommendations at overseas locations where AFRC operates, and where no other assessment is published by AMC or other organization.

1.4.2. The weekly TWG briefings cover the following areas:

1.4.2.1. Threat Information (OPR: AFOSI/DOIO).

1.4.2.2. Operational Information (OPR: DOOM).

1.4.2.3. Security Environment (airfield, billeting, etc.) (OPR: AFOSI Region 3/ OL-B&AFRC/SFO).

1.4.2.4. TWG Recommendations (OPR: TWG).

1.4.3. TWG products are sent electronically to AFRC units at home station and are available on INTELINK-S.

1.4.4. Aircrew debriefing, MISREPS and Phoenix Raven Team post-mission reports provide feedback to the TWG on security risks to missions and force protection issues.

2. Headquarters AFRC Responsibilities:

2.1. Intelligence and Information Operations Division (DOI):

2.1.1. Serves as AFRC's office of primary responsibility (OPR) and Director of the TWG.

2.1.2. AFRC/DOIO is the focal point for all intelligence analysis, planning, direction, exploitation, production, and dissemination of intelligence to support the TWG processes.

2.1.3. Provides senior leaders immediate analysis on critical information potentially impacting on-going AFRC missions.

2.1.4. Provides current imagery, maps, and other current intelligence products.

2.1.5. Provides editing and production assets required to construct risk assessment briefings and products.

2.1.6. Provides situational awareness briefings to the TWG in the form of current intelligence briefings.

2.1.7. Monitors the secure launch (that is, AMC, USAFE) report to identify airfields requiring updated risk assessments, imagery, and database maps to ensure adequate force protection measures are in place prior to mission execution.

2.1.8. Places select TWG products on-line via INTELINK-S to ensure widest dissemination to AFRC units.

2.1.9. Represents TWG in daily operations tempo meeting and validates force protection recommendations for the following day's scheduled missions.

2.1.10. Action officers participate, as required, in cross-functional briefings for AFRC/CC/CV and senior staff.

2.2. Director of Security Forces (SF):

2.2.1. Assesses adequacy of supported command force protection and security policies to provide adequate protection for AFRC resources.

2.2.1.1. Assesses adequacy of force protection and security of AFRC missions.

2.2.2. Ensures force protection initiative guidance is included in applicable security force directives.

2.2.3. Develops force protection and personnel protection guidance for inclusion in TWG risk assessments.

2.2.4. Ensures Raven Team taskings are forwarded to the appropriate DOOM planners for inclusion in the Global Decision Support System (GDSS).

2.2.5. Provides TWG action officers Raven Team post-mission reports.

2.2.6. Action officers participate, as required, in cross-functional briefings for AFRC/CC/CV and senior staff.

2.3. Command Center (OPR: DOCC):

2.3.1. DOCC ensures command and control issues related to TWG processes and force protection issues are adequately addressed in TWG meetings.

2.3.1.1. Participates as DOC representatives to the TWG.

2.3.1.2. Monitors on-going AFRC missions.

2.3.1.3. Engages other DOC offices and processes required to facilitate TWG issues and tasking. Provides insight regarding DOC internal processes and players affecting or affected by TWG decisions and products.

2.3.1.4. Contacts on-call TWG representatives during non-duty hours.

2.4. AFOSI Region 3/OL-B:

2.4.1. The primary mission of AFOSI Region 3/OL-B is to provide counterintelligence support within AFRC. As a member of the TWG, AFOSI Region 3/OL-B advises the TWG on antiterrorism and counterintelligence issues (collection, investigation or counterespionage-related matters).

2.4.2. Provides the TWG the latest threat information available on terrorism, crime, and foreign intelligence.

2.4.3. Action officers participate, as required, in cross-functional briefings for AFRC/CC/CV and senior staff.

2.4.4. Develops personnel protection guidance for inclusion in TWG risk assessments.

2.5. Current Operations Division (DOO):

2.5.1. AFRC/DOOM and DOOX participate in the TWG as the representatives for the Current Operations Division.

2.5.2. The DOO representative ensures current operations issues related to TWG processes and force protection are addressed in daily TWG meetings.

2.5.3. Engages other DOO offices, as required, to facilitate TWG issues and tasking. Provides insight regarding DOO internal processes and organizations affecting or affected by TWG decisions/products.

2.5.4. Provides the TWG current mission schedules.

2.5.4.1. Screens all mission identifier (MI) requests for Phoenix Raven required locations and notifies SFOF.

2.5.5. Action officers assigned to DOO participate, as required, in cross-functional briefings for AFRC Staff.

2.5.6. DOOX identifies Chairman of the Joint Chiefs of Staff (CJCS) exercise and contingency requirements to the TWG to include mission support force deployments, airlift flow, level of play, and any other unique requirements.

2.5.6.1. Provides CJCS exercises and contingency operational information for TWG Briefings.

2.5.6.2. Provides a monthly projection for CJCS exercises and contingencies requiring TWG assessments and recommendations.

2.6. Directorate of Health Services (SG): The AFRC/SG provides the TWG medical-related information that could potentially impact deployed AFRC personnel.

3. WING/GROUP, Direct Reporting Unit (DRU) and Geographically Sepa rated Unit (GSU) Level Responsibilities:

3.1. Requirements. Minimum requirements for establishing and maintaining the TWG program at the unit level are:.

3.1.1. Each wing/group, DRU, and GSU should convene a TWG to review force protection issues relating to assigned AFRC missions. The unit commander may also convene a TWG as deemed necessary based on the local security situation and directives.

3.1.2. The TWG membership, as a minimum, should include representatives from operations, intelligence, AFOSI, and security. Coordinate with supporting AFOSI and Security Forces when membership is not available.

3.2. Responsibilities:

3.2.1. Review appropriate HQ AFRC TWGs risk assessments and force protection recommendations.

3.2.2. Evaluate local threat situation as appropriate.

3.2.3. Develop and document procedures to implement HQ AFRC TWG Force Protection recommendations.

3.2.4. Produce timely MISREPS according to GMAJCOM requirements to assist local and HQ level TWGs better assess in-place force protection measures and determine the need for additional force protection requirements and actions.

3.2.4.1. Send completed MISREPS to AFRC/DOI.

3.2.4.2. Request/coordinate force protection issues with HQ AFRC TWG members.

JAMES E. SHERRARD III, Maj Gen, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

Abbreviations and Acronyms

AAFIF—Automated Air Facility Intelligence File

AFI—Air Force Instruction

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFSOC—Air Force Special Operations Command

AFRC—Air Force Reserve Command

AFRCI—Air Force Reserve Command Instruction

AMC—Air Mobility Command

AME—Air Mobility Element

AMMP—Air Mobility Master Plan

AOR—Area of Responsibility

AT—Antiterrorism

CI—Counterintelligence

CIA—Central Intelligence Agency

CJCS—Chairman, Joint Chiefs of Staff

CMW—Compartmented Mode Workstations

COMSEC—Communications Security

CONOPS—Concept of Operations

CSG—Cryptologic Support Group

CSS—Central Security Service

CT—Counterterrorism

DAO—Defense Attaché Office

DCI—Director of Central Intelligence

DHS—Defense HUMINT Services

DIA—Defense Intelligence Agency

DoD—Department of Defense

DoDD—Department of Defense Directive

DRU—Direct Reporting Unit

DS—Defensive Systems

EEI—Essential Elements of Information

FAA—Federal Aviation Administration

FP—Force Protection

GDSS—Global Decision Support System

HUMINT—Human Resource Intelligence

I&W—Indications and Warning

IIR—Intelligence Information Report

IMINT—Imagery Intelligence

IN—Chief of Intelligence (Air Force, MAJCOM, Wing, Group)

INCR—Intelligence Conference Room

INTELINK-S—Intelligence Link (a secure "internet" for classified information)

INFOSEC—Information Security

IO—Information Operations

IW—Information Warfare

J2—Director of Intelligence

JCS—Joint Chiefs of Staff

JIC—Joint Intelligence Center

JWICS—Joint Worldwide Intelligence Communications System

MANPADS—Man Portable Air Defense System

MC&G—Mapping, Charting and Geodesy

MI—Mission Identifier

MISREPS—Mission Reports

MOG—Maximum on Ground

NIMA—National Imagery and Mapping Agency

NPIC—National Photographic Interpretation Center

NRO—National Reconnaissance Office

NSA—National Security Agency

OL—Operating Location

OPLAN—Operations Plan

OPORD—Operations Order

OPR—Office of Primary Responsibility

OPSEC—Operations Security

RFI—Request for Information

RON—Remain Over Night

RSO—Regional Security Officer

SCI—Sensitive Compartmented Information

SIGINT—Signals Intelligence

SITREP—Situation Report

SF—Security Force

TACC—Tanker Airlift Control Center

TALCE—Tanker Airlift Control Element

TSR—Time Sensitive Requirement

TTF—Tanker Task Force

TWG—Threat Working Group

USSS—United States SIGINT System

VTC—Video Teleconference

Terms

Antiterrorism—Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

Counterintelligence—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

Counterterrorism—Offensive measures taken to prevent deter and respond to terrorism.

Information Warfare (IW)—IW is action taken to deny, exploit, corrupt, or destroy an adversary's information, information systems, and information operations, while protecting friendly forces against similar actions.

Operations Security (OPSEC)—A process identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to identify those actions that can be observed by adversary intelligence systems; determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together critical information in time to be useful to adversaries; or select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

PHOENIX RAVEN TEAM—Two to four person "Fly-Away" Security Team tasked with providing close-in security for AFRC aircraft at OCONUS areas where the local security has been assessed as inadequate or the security situation is not fully known.

Attachment 2

RELATED THREAT WORKING GROUP PUBLICATIONS

Joint Publication 1-02--*DoD Dictionary of Military and Associated Terms*

Joint Pub 3-07-2--*Joint Tactics, Techniques, and Procedures for Antiterrorism*

USTCH 31-2--*Security Awareness Guide to Combating Terrorism*

AFPD 10-11--*Operations Security*

AFI 14-105--*Unit Intelligence Mission and Responsibilities*

AFPD 31-1--*Physical Security*

AFPD 31-4--*Information Security*

AFPD 71-1--*Criminal Investigations and Counterintelligence*

AFI 10-1101--*Operations Security*

AF131-207--*Arming and Use of Force by Air Force Personnel*

AFI 31-210--*The Air Force Antiterrorism/Force Protection (AT/FP) Program Standards*

AFI 31-401--*Information Security Program Management*

AFI 31-501--*Personnel Security Management Program*

AFI 31-601--*Industrial Security Program Management*

AFI 31-702--*System Security Engineering*

AFI 31-703--*Product Security*

AFI 71-101, Volume 1--*Criminal Investigations*

AFJI 31-102--*Physical Security*

AMCI 14-102--*Debriefing and Reporting* (attachment)

AMCI 31-104--*Phoenix Raven Program*

Director of Mobility Forces (DIRMOBFOR) Handbook

Attachment 3

AIR FORCE RESERVE COMMAND’S FORCE PROTECTION ESSENTIAL ELEMENTS OF INFORMATION

1. When conducting an airfield survey, use the following questions to complete your report. Your report should be in paragraph format, explaining the questions in as much detail as possible. Those items identified by an asterisk (*) are considered critical information to be included in your report.

2. Airfield Name/Location:____________________ ICAO____________ Date: ________

2.1. FENCING/WALLS

Is the airfield perimeter completely fenced or walled (type, height, condition, gaps, holes, etc)?

Is the flightline/ramp fenced? Describe (type, height, condition, gaps, holes, etc)?

Are there clear zones on each side of the fence/wall?

Is the airfield perimeter or flightline area posted "No Trespassing" or "No Admittance"?

2.2. OTHER PHYSICAL BARRIERS

List different types, locations and numbers of barriers used on the perimeter and on/near the flightline/ramp.

Is the airfield or aircraft parking area under closed circuit TV (CCTV)?

2.3. SECURITY FORCE LEVEL

How many guards are typically on duty during the day and night?

Are these guards host military units? Police or security police? Or contract personnel?

To what extent and for how long can this force be augmented by in-place/nearby personnel?

Shift duration and shift change procedures/times.

What local customs might result in decreased security (e.g. national holidays, traditional daily rest periods, etc)?

2.4. SECURITY PERSONNEL

Are personnel well trained and professional (does this vary by position; are the supervisory personnel better trained or more motivated)?

What factors make individual members or groups susceptible to blackmail/bribery (e.g. low pay, irregular pay, mistreatment by senior leadership, etc.)?

What is the predominant language/dialect spoken by security forces (also indicate what percentage speak English, if applicable)?

To what degree are they willing to work with US/Allied personnel?

Are security forces willing/able to provide increased security for US/Allied missions?

If so, how are such arrangements made? Through DAO office?

2.5. PATROLS

Is the perimeter and/or flightline controlled by armed guards?

Frequency and regularity of patrols. (Are the patrols conducted on a predictable schedule or are they conducted randomly by the airport security force? If not on a regular schedule, is the variance purposeful (i.e. a security measure)?

Is patrol made on foot, animals, or vehicles?

How many people are on each patrol?

Do patrols use military working dogs (MWD)?

2.6. SECURITY EQUIPMENT

What types of weapons do guards carry?

What additional weapons are available (what weapons can be used, if needed; what weapons are used on vehicles, at entry points, guard towers, etc.)?

What forms of communications gear do the security personnel use?

2.7. WATCH TOWERS/FIXED GUARD POSITIONS

Number, location and description (ground level guard shack, elevated tower, fixed fighting positions/bunkers, etc.)?

Number of guards at each location?

2.8. QUICK REACTION/COUNTERTERRORIST UNITS

Does such a force exist?

Is it on or near the airport?

What is its reaction time?

How large a force is it?

To what degree is responsibility delegated in crisis situations?

How is the force trained and equipped?

Does it have higher morale than the regular guard forces?

Has it successfully conducted operations in the past?

2.9. ENTRY CONTROL POINTS (ECPs)

Is entry controlled to the installation and flightline/ramp?

Number, location and description of ECPs at the perimeter and flightline/ramp areas.

Are gates locked if unmanned?

Number of guards at each entry point (military/civilian, airport police, day/night).

Are x-ray machines and /or metal detectors used at any of the entry points?

If entry is controlled, what form(s) of personal identification are required for individuals and vehicles?

Are private vehicles allowed?

If so, what method of registration is required?

Are all persons in a vehicle required to show identification?

What are visitor control procedures (i.e., procedures for visitor approval, identification of same)?

What are visitor escort procedures?

To what degree are vehicles, personnel and their possessions searched?

Do any of the above procedures vary at night (i.e., all personnel must show identification at night when entering the installation, etc.)?

2.10. LIGHTING

Is the entire boundary, flightline, and parking ramp lighted at night?

Are additional fixed spotlights located at watchtowers/entry points?

Are mobile mounted/towable spotlights available?

2.11. PARKING

Are US Government aircraft parked in special locations?

If so, are additional guards posted?

Is the area clearly marked as a restricted area?

Are US personnel authorized to have weapons on the flightline/ramp?

Are weapons storage facilities available to transient crews?

3. LODGING (use when AFRC aircraft must remain over night at foreign airfields)

Does AMEMBASSY provide lodging in its compound?

If lodging is unavailable at the compound, does AMEMBASSY/DAO maintain a list of hotels that meet minimum security requirements?

If EMBASSY maintains a standing list of recommended hotels, request the following information on each if available:

Basic description (design, height, towers, interior/exterior entrances, number of rooms)

General layout (parking areas, fencing, lighting, proximity to highways/major roads)

Number of elevators/stairways (internal/exterior), building entrances/exits, vehicle entrances/exits.

Are US personnel lodged in the same areas of the hotel or are they separated?

How is the crew transported to and from the hotel?

Are metal detectors/x-ray machines used at hotel entrances?

Are security forces available to escort crews transiting to/from airport?

4. OFF-INSTALLATION ROUTE SECURITY (use when AFRC aircraft must remain over night at foreign airfields)

Distance from airport to hotel.

Number of different routes from airport to hotel.

Route description(s).

Choke points on route (to include excessive traffic lights, congestion)

Number of lanes each way.

One-way streets?

Number and location of safe houses (i.e., police stations) along route.

Does host nation regularly patrol these routes?

Any bridges, overpasses or tunnels along the route?

5. PERSONNEL THREAT

Are dissidents known to operate in the area of the airport?

Identify these groups by name with leaders if known.

Are dissidents known to possess stand-off weapons (SAMS, RPG, mortar, etc., (specific type and any known modification))

Are these groups known to possess communications monitoring equipment (identifying type and capability if known)?

Are these groups known to have anti-US sentiments?

What past incidents have occurred where US personnel, equipment, facilities were targeted?

Do hostile elements have any specific times/dates when they are historically active?

Do they have the support of the local populace?

6. PHYSICAL LOCATION

What natural/manmade obstacles are in the vicinity of the airport (e.g., power lines, tall buildings, etc.)?

Identify areas surrounding flightline parking which could be used by hostile elements to covertly surveil airport operations and to launch attacks?

How suitable is the surrounding terrain and vegetation for a standoff attack? Does this vary seasonally?

7. MAPS/CHARTS

Please include maps or a sketch locating security information (aircraft parking areas, fencing, lighting, ECPs, etc.). Digital photos of all items are requested, if capability exists.

8. FINAL

When complete, send your report to HQ AFRC/SFO, DSN FAX 497-0103, or send by E-mail to the OPR at__________@AFRC.af.mil Any questions can be addressed to HQ AFRC/SFO at DSN 497-0106/ 0105.

Attachment 4

SAMPLE

AFRC THREAT WORKING GROUP (TWG) AIRFIELD RISK ASSESSMENT AFRC THREAT WORKING GROUP (TWG)

Valid as of XX XXX 2000

SUBJECT: XXXXXX Airfield, XXX Country (ICAO) Risk Assessment (U)

LOCATION:

(U) General Location: 8 miles south of capital city.

(U) This section will give a general location for the airfield relative to a major city and may provide coordinates.

TERRORIST THREAT: *-AOR-*

(U) Terrorist threat to American interests in the XXX (country) is HIGH.

(U) This section will describe capabilities, intent, and history of terrorist groups to target or observe US citizens or assets within the country.

(U) Provides information on modus operandi of the known terrorist groups within the country.

(U) Gives details on any recent specific terrorist attacks on US citizens and assets.

MILITARY THREAT: *-AFRC/DOI-*

(U) The military threat to AFRC air and ground operations is LOW.

(U) This section will provide information on the history or intent of the host nation military or the regional militaries to target US or allied assets.

(U) Provides details on any recent specific encounters between host nation/regional militaries with USAF assets.

CRIMINAL THREAT: *-AFOSI-*

(U) The criminal threat to AFRC aircrew/personnel in Kuwait is LOW.

(U) This section provides information on crimes that occur routinely within the country or region with special attention to the airfield and its vicinity.

(U) Gives an idea of what serious crimes could occur in the region.

(U) Discusses availability of weapons to criminal elements, problems stemming from drug trafficking, and similar issues.

(U) Discusses measures US personnel should take to avoid becoming a victim of crime.

(U) Advises on most secure lodging options available and route security concerns between the airport and lodging.

FOREIGN INTELLIGENCE THREAT: *-AFOSI-*

(U) There is no evidence country XXX's intelligence services are actively targeting US assets.

(U) This section will provide specifics on what intelligence services (host-nation and regional) are specifically targeting US personnel and what their priority is on collection that information.

(U) Provides capability to collect information and modus operandi of collection practices.

THREAT MITIGATING TACTICS: *-AFRC/DO-*

(U) The most important operational threat to operations into XXX airfield is XXX. Take the following measures to mitigate that threat:

(U) This section will cover tactics recommended to counteract potential threats to AFRC operations.

INFORMATION OPERATIONS THREAT: *-AFRC/DOI-*

(U) The most vital information operation threat to AFRC assets is XXX.

(U) This section will discuss specifics on host nation entities and others who have the capability or intent of using information operations to target US forces.

(U) Covers any targeting of government computers, phone lines, monitoring of friendly mission-related information (OPSEC), psychological operations employed by the enemy, etc.

MEDICAL THREAT: -AFRC*/SG-*

(U) The most pressing medical concern at XXX airfield is XXX.

(U) As applicable, this section covers any medical concerns with endemic diseases and what actions US personnel should take to prevent those diseases.

(U) Discusses sanitary conditions at the airfield/in the country and practices that should be taken to mitigate the speed of disease.

(U) May cover climate concerns and what should be done to prevent hypothermia, dehydration, etc.

(U) Covers host nation medical treatment facilities/capabilities and the location of US-run medical facilities within the country.

AIRFIELD SECURITY: *-AFRC/SF-*

(U) The airfield security at airfield XXX is considered good.

(U) This section will provide an overview of the security at and around XXX airfield.

(U) Provides specifics on fencing, lighting, entry control points, line badge system, and security forces responsible for patrolling the airfield, including their effectiveness in addition to other specifics on airfield security.

DS EQUIPPED	ARMOR	MOG OF ONE	DAYLIGHT OPS ONLY	NIGHT OPS ONLY	NO RON	RAVEN REQUIRED
MEP*		X@			X	

*Maximum extent possible**X** @: Deviation requires CV approval**X**: Deviation requires AFRC/DO approval

___________	___________	___________	___________	___________	___________
AFRC/DOI	AFRC/DOO	TACC/XOC	AFRC/SF	AFOSI	AFRC/DOT

Name/Ofc Sym/ext/initials/Date

CLASSIFIED BY: XXXXXX

DECLASSIFY ON: XX XXX XX

Attachment 5

STANDARD COUNTERMEASURES (OPR)

Table A5.1. Standard Countermeasures (OPR)

STANDARD COUNTERMEASURES (OPR)
A. Negligible threat location; no specific force protection measure required
B. Reserved for later use
C. Criminal threat exists – enforce personal protection measures (UNIT OG/CC)
C1. Petty theft, street crime; travel in groups, wear civilian clothes off base, & avoid high risk areas (Unit OG/CC)
C2. High crime area (muggings, car-jacking, armed robberies); minimize activities after dark (in addition to C1)(Unit OG/CC)
C3. Extreme violent crime present; stay in hotel or on base (Unit OG/CC)
D. Manpad threat exist; employ aircraft defensive systems (AFRC/DOOM Unit OG/CC)
E. Reserved for later use
F. Poor airfield lighting & security; restrict airfield operations to daylight hours only (Unit OG/CC)
G. Poor security for acft & personnel; no remain overnight (RON) (Unit OG/CC)
H. Poor security for acft & personnel; minimize ground time (Unit OG/CC)
I. Incomplete assessment, more research required (TWG)
K. Threat on airfield exists; arm crewmembers (Unit OG/CC)
M. USAFE TWG item: medical advisory-additional immunizations personal protective equipment medications and listed in the comments
M1. USAFE TWG item: local community food and/or water not safe-drink only sealed water and eat only food served hot
M2. USAFE TWG item: upper respiratory disease threat-meningococal immunizations required, consult immunizations
M3. USAFE TWG item: disease carrying insects present-use insect repellant (DEET), wear long sleeve shirts, no shorts
M4. USAFE TWG ITEM: malaria threat-anti-malarial medications required, consult flight surgeon
O. Hostile foreign intelligence (FIS) threat exists – maintain good OPSEC (Unit OG/CC)
O1. Medium FIS threat – be aware that Americans have been targeted (Unit OG/CC)
O2. High FIS threat – expect surveillance & monitoring of phones hotel rooms and taxis (Unit OG/CC)
O3. Critical FIS threat – expect exploitation by FIS (Unit OG/CC)
Q. Reserved for later use
R. Airfield security is poor – deploy MST or coordinate local security for aircraft

R1. Assign AFRC Raven team (AFRC/SF, Unit OG)
R.2. Arrange local security for aircraft (AFRC/SF, Unit OG)
T. Terrorism threat exists – maintain low profile (Unit OG/CC)
T1. Americans are not direct targets – avoid demonstrations, public transportation sites (Unit OG/CC)
T2. Americans are direct targets – avoid all public areas and high risk establishments when possible (Unit OG/CC)
T3. Known or suspected targeting of airfield (Unit OG/CC)
U. Unrest and civil disorder exists – maintain low profile (Unit OG/CC)
X. Threat situation presents danger to aircraft personnel – cancel mission (AFRC/DOOM/DOOX)
X1. Contact sponsor to restrict MOG (AFRC/DOOM/DOOX)
X2. Contact sponsor to move mission/deployment base (AFRC/DOOM/DOOX)
X3. Contact sponsor to modify mission deployment schedule (AFRC/DOOM /DOOX)
X4. Contact sponsor to enhance airfield security (AFRC/SF/DOOX)
X5. Contact sponsor to vary arrival and departure times (AFRC/DOOM/DOOX)
X6. Contact sponsor to restrict airfield ops to day only (AFRC/DOOM/DOOX)
X7. Carry aircrew ensemble (AFRC/DOOM and Unit CC/OG/LG)
X8. Provide deploying troops personal weapons (Unit CC/LG)
X9. Carry ground crew ensemble (AFRC DOOM DOOX and Unit CC/CE/LG)
X10. Provide mission/deployment troops with body armor (AFRC DOOM DOOX and Unit CC/LG)
Y. Raise THREATCON at threatened AFRC base (AFRC/DO/SF and Unit CC/OG)
Z. Provide the unit a special risk assessment and/or force protection information (AFRC/DOIO/SF/FIR 3 OL-B)
Z1. Rebrief troops on personal counter-terrorism protective measures (Unit CC/SF)
Z2. Rebrief troops on foreign intelligence threat (Unit CC/SF)
Z3. See additional countermeasures listed in paragraph 4
Z4. See additional comments listed in paragraph 5

Attachment 6

SAMPLE MANPAD THREAT ASSESSMENT MATRIX

Figure A6.1. Sample MANPAD Threat Assessment Matrix

Airfield MANPAD Threat Assessment: ____________________

Factors (OPR)	A	B	C	D	E
1. MANPAD Availability for Hostile Elements (IN/OSI)	MANPAD presence highly unlikely	Potential of MANPADs in the country	Specific reporting of MANPADs in country, source credibility undetermined	Specific reporting of MANPADs in country, credible source/multiple sources	Confirmed evidence of MANPADs in the country
	0	5	10 14	15 20	25
2. Intent to Carry out MANPAD Attack (Actual MANPAD use warrants additional assessment) (IN/OSI)	No assessed intent to use MANPADs and negligible likelihood that MANPADs are possessed by opposition groups	No assessed intent to use MANPADs but likelihood exists that MANPADs are possessed by opposition groups	Assessed intent to use MANPADs and slight likelihood that MANPADs are possessed by opposition groups	Assessed intent to use MANPADs and moderate likelihood that MANPADs are possessed by opposition groups	Assessed intent to use MANPADs and high likelihood that MANPADs are possessed by opposition groups
	0	5	11 20	21 40	50
STOP: If Total Score of Factors 1 and 2 is 20 or Less, NO DS Requirement; NO additional assess is required					
3. Internal Security	Excellent Internal Security	Good Internal Security	Moderate Internal Security	Undetermined/poor Internal Security	Critical Internal Security
	-15	-10	0	10	15
4. Terrorist Threat (IN)	Negligible	Low	Medium	High	Critical
	0	5	15	25	35
5. Military Threat (IN)	Negligible	Low	Medium	High	Critical
	0	5	15	25	35
6. Government Stability/Regional Political Tensions (IN)	No open conflict or tangible intent to destabilize the government	No open conflict; Opposition group has destabilizing influences	Intermittent conflict in the region and/or government involved in occasional skirmishes with opposition group(s)	Open armed conflict in immediate region and/or gov't engaged in persistent conflict with opposition group(s)	Open armed conflict in the immediate region and/or government facing serious threats to survival.
	0	5	10	15	20
7. Security of MANPAD Footprint (SF/OSI)	MANPADS footprint closely monitored by US/Host Nation Military Personnel (open terrain)	MANPADS footprint closely monitored by Host Nation Military/Civilian police (open terrain)	MANPADS footprint closely monitored by US/Host Nation Military/Civilian police (rugged or urban terrain)	Daily random day and night patrols of MANPADS footprint by host nation military/ civilian police (rugged or urban terrain)	No Exterior Security or Patrolling
	-25	-5	0	10	25
8. Mission (Frequency, predictability, profile) (TACC)	Low mission frequency, unpredictable, and low profile	Moderate mission frequency, unpredictable, and low profile (1 of 3)	Moderate mission frequency, unpredictable, and low profile (2 of 3)	Moderate mission frequency, unpredictable, and low profile (3 of 3)	High mission frequency, highly unpredictable, and high profile
	-10	0 4	5 15	16 25	30
0-70 points. No DS requirements.	**71-110** points. Use DS to Max Extent Possible. No approval required to waive use of DS.	**111-145** points. Use DS to Max Extent Possible. TACC/CC approval to waive requirement.	**146+**. All missions require use of DS. AFRC/CC or AFRC/CV approval to waive requirement.	**Total for This Airfield (Max Possible Score: 235)**	
Mitigating Factors	Ability to use blacked out operations, or terrain masking, or TAA/D (all 3 applicable)	Ability to use blacked out operations, or terrain masking, or TAA/D (any 2 of 3 applicable)	Ability to intermingle commercial and military aircraft at night (not used in conjunction with tactics)	Ability to use blacked out operations, or terrain masking, or TAA/D (any 1 of 3 applicable)	No mitigating factor
	-25	-15	-10	-5	0

Attachment 7

SAMPLE THREAT MATRIX ASSESSMENT

Figure A7.1. Sample Threat Matrix Assessment.

If Mission Profile and MANPAD Vulnerability is High, Consideration of Additional Steps to Mitigate the Threat Should be Considered

ICAO:	AFRC THREAT WORKING GROUP OPERATIONAL RISK ASSESSMENT	RAVEN REQUIRED: YES / NO

NAME/LOCATION OF AIRFIELD: **DATE ASSESSED:**

DATA SOURCE:

The criminal threat is:	Negligible: 0 Points	Low: 5 Points	Medium: 15 Points	High: 25 Points	Critical: 35 Points
The Terrorist Threat is:	Negligible: 0 points	Low: 10 points	Medium: 20 points	High: 30 points	Critical: 35 points
The Military Threat is:	Negligible: 0 Points	Low: 0 Points	Medium: 20 Points	High: 60 Points	Critical : 95 Points
FACTORS	0 POINTS	5 POINTS	10 POINTS	15 POINTS	20 POINTS
Installation/airport security services are:	provided by US military	Host nation or contract security, reliability is not in question	host nation or contract security, reliability is unknown	Host nation or contract security, reliability is in question	No organized security available
Host security forces control entry:	Via a manned installation entry point and a credential check for flightline access	to the flightline only	to the installation/airport only	to neither the flightline or installation/airport	
There is perimeter fencing or barriers around:	the flightline & installation/airfield perimeter	the flightline only	to the nstallation/airfield perimeter only	none available	
Security forces will _____ security incidents involving the aircraft.	provide US area patrol and 5 minute armed response (AFI 31-101 standards)	provide armed response to	provide unarmed response to	notify the aircraft commander or civilian authorities of	
The aircraft will be parked:	in a US military aircraft only parking area	separate from host military and civilian acft	among other host military aircraft only	among other civilian aircraft	
Illumination will:	be area and perimeter lighting	be area lighting only	be perimeter lighting only	No lighting available	
Security measures at billeting are: (Consider if RON)	on base or within US government facility	surveillance of entry/exit with armed security	security personnel (armed or unarmed) on duty 24 hours	non-existent	
Routes of travel between the airfield and billeting are: (Consider if RON)	multiple routes with negligible vulnerabilities	multiple routes with contract drivers or escort	multiple routes with some vulnerabilities without assigned driver or escort	single/multiple route with vulnerabilities without assigned driver or escort	
GRAND TOTAL:					

5			20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120	125	130	135+

MAINTAIN AWARENESS **CONSIDER MITIGATING MEASURES** **CONSIDER CANCELLING MISSION**

(135+ - STRONGLY CONSIDER CANCELLING MISSION)